500,797

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
31 juillet 2003 (31.07.2003)

PCT

(10) Numéro de publication internationale
WO 03/063099 A2

(51) Classification internationale des brevets[7] : G07F

(21) Numéro de la demande internationale :
PCT/CA03/00049

(22) Date de dépôt international :
16 janvier 2003 (16.01.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
2,367,309 17 janvier 2002 (17.01.2002) CA
2,394,742 7 août 2002 (07.08.2002) CA

(71) Déposant et
(72) Inventeur : CARON, Michel [CA/CA]; 196, rue Michel Duguay, Varennes, Québec J3X 1J5 (CA).

(74) Mandataire : OGILVY RENAULT; Suite 1600, 1981 McGill College Avenue, Montreal, Québec H3A 2Y3 (CA).

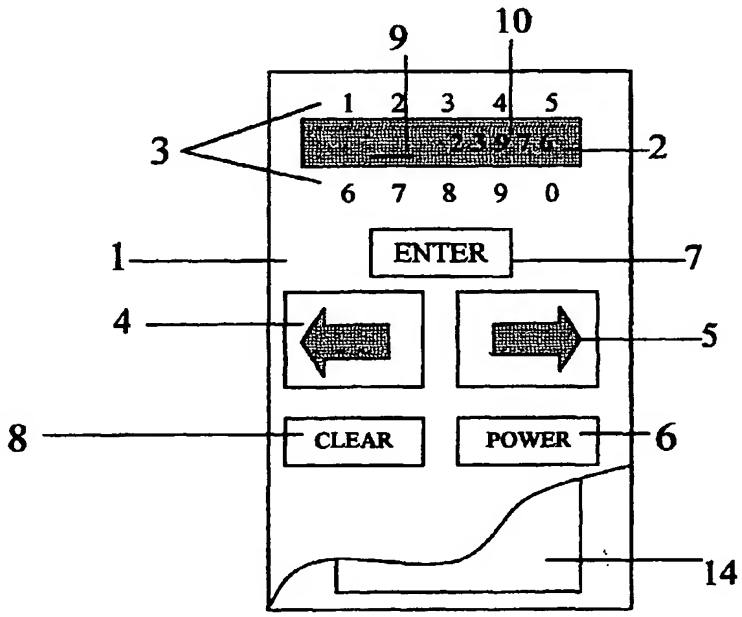
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR),

[Suite sur la page suivante]

(54) Title: APPARATUS AND METHOD OF IDENTIFYING THE USER THEREOF BY MEANS OF A VARIABLE IDENTIFICATION CODE

(54) Titre : APPAREIL ET PROCÉDÉ PERMETTANT D'IDENTIFIER SON UTILISATEUR AU MOYEN D'UN CODE D'IDENTIFICATION VARIABLE



(57) Abstract: The invention relates to an apparatus (1) and a method (100) which form a universal identification means for a user party. According to the invention, the user can be identified with respect to one of numerous second parties. The inventive apparatus consists of: a data entry device (4, 5, 7, 8, 9, 11, 12, 13 and 15); a device for selecting the second party (4, 5, 7, 8, 9, 12, 13, 15) from numerous second parties in relation to which said user party can be identified; a data output device (2, 15); and a data processing device (14) comprising a storage device and an algorithm (60, 70) that can be used to generate a variable identification code (10), which is specific to a given use by the user party, and to disclose said code using the data output device (2, 15).

(57) Abrégé : L'appareil (1) et la méthode (100) , sont un moyen d'identification universel pour la partie utilisatrice. L'identification de l'utilisateur peut se faire auprès d'une de plusieurs secondes parties. L'appareil comprend un dispositif d'entrée de données (4, 5, 7, 8, 9, 11, 12, 13 et 15), un dispositif de sélection de la seconde partie (4, 5, 7, 8, 9, 12, 13, 15) parmi une pluralité de secondes parties auprès desquelles ladite partie utilisatrice peut s'identifier, un dispositif de sortie de données (2, 15) et un dispositif de traitement de données (14) comprenant un dispositif de mémorisation et un algorithme (60,70) permettant de générer un code d'identification variable (10) spécifique à une utilisation donnée par la partie utilisatrice et de le révéler au moyen dudit dispositif de sortie de données (2,15).

WO 03/063099 A2

brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

APPAREIL ET PROCÉDÉ PERMETTANT D'IDENTIFIER SON UTILISATEUR AU MOYEN D'UN CODE D'IDENTIFICATION VARIABLE

DOMAINE DE L'INVENTION

La présente invention concerne le domaine des appareils et procédés permettant à une partie utilisatrice de s'identifier formellement auprès d'une seconde partie parmi une pluralité de secondes parties. Plus spécifiquement, l'invention concerne un processus universel d'identification et un appareil électronique permettant à un utilisateur unique auquel il est dédié de s'identifier formellement auprès d'une de plusieurs secondes parties.

HISTORIQUE DE L'INVENTION

Depuis toujours l'usurpation d'identité a été un grave problème dans la société. Les cartes d'identités ont été créées pour résoudre cette problématique. Même imparfaite cette solution a tout de même permis de réduire l'ampleur de ce problème. Mais bien vite la contrefaçon des pièces d'identités s'est développée. Le vol de cartes de crédit s'est également étendu à grande échelle, entraînant des pertes de plus en plus considérables pour le système financier international. L'introduction des cartes de débit avec un numéro d'identification personnel (NIP) a permis aux banquiers d'avoir une longueur d'avance sur les fraudeurs. Mais ce ne fut qu'une question de temps avant que ces derniers trouvent un moyen de tromper le système. C'est maintenant fait depuis quelques années. Il importe pour la sécurité physique et financière de tous de recourir à des moyens plus efficaces d'enrayer ce fléau. En outre, on reconnaît l'importance d'un moyen efficace d'identification pour non seulement éliminer une très grande partie des fraudes effectuées avec des cartes de crédit et de débit, mais également permettre à d'autres organismes adhérents, tel que services gouvernementaux, employeurs, etc., d'identifier formellement leur usager, client ou employé même et surtout, si celui-ci se trouve à distance.

Il existe quelques demandes de brevets (US5317636, WO9964956, US4849613, US5130519, US6247129, US6163771, US4697072, US5311594, US5485519) qui ont été déposées et/ou obtenues pour des procédés concernant l'authentification d'un client d'une carte de paiement, dans le cadre de transactions commerciales. Tous ces procédés et appareils, mêmes s'ils sont inventifs, sont

dépourvus, de certaines caractéristiques qui leurs permettraient de combler tous les besoins d'identification de leur détenteur.

Les appareils et procédés connus à ce jour sont conçus pour identifier le détenteur d'une carte de paiement, alors qu'il est souvent nécessaire à une personne de s'identifier auprès de plusieurs organismes dans un contexte différent de celui d'une transaction commerciale impliquant l'utilisation d'une carte de crédit ou de débit.

Il existe déjà sur le marché des logiciels pour la fourniture d'un numéro unique lors de transactions sur Internet avec une carte de crédit ou encore pour avoir accès à des banques de données hautement sécuritaires. Il y a également sur le marché, un petit appareil portatif qui affiche continuellement sur son écran, un code différent à intervalle régulier soit aux 30, 45 ou 60 secondes. Ce code est généré à l'aide d'un algorithme intégré au microprocesseur de cet appareil. Un serveur informatique ayant le même algorithme peut vérifier l'authenticité de la personne en lui demandant de fournir ce code à tout moment lors d'une communication. La plupart du temps la transmission de ce code se fait lors de la connexion audit serveur. Mais cet appareil ne sert qu'à un site et n'est pas totalement sécuritaire, le code étant constamment visible à l'écran, quiconque ayant l'appareil en main peut alors l'utiliser en se faisant passer pour le détenteur légitime.

Beaucoup d'innovations ont été proposées pour l'inclusion d'un générateur de numéro aléatoire à même la carte de crédit ou de débit. Le problème que cela entraîne est un peu du même ordre que celui que nous venons de décrire : une personne qui n'est pas le détenteur de la carte peut tout de même transiger avec une carte qu'elle aurait dérobée, car le code est transmis la plupart du temps par une puce électronique qui est lue par un lecteur. Puisque des lecteurs de cartes à puce doivent être implantés un peu partout, cela augmente également de façon considérable le coût d'implantation d'un tel système. Et ces procédés ne sont d'aucune utilité dans les endroits ne disposant pas de tels lecteurs. Les transactions sur Internet sont également exclues de procédés semblables, à moins qu'elles ne soient effectuées sur des ordinateurs équipés d'un tel lecteur de cartes à puce.

Une autre difficulté avec les innovations précédentes est l'introduction de la «variable temps » dans l'algorithme qui génère le code unique. Pour que cela soit facile et rapide d'utilisation, il faut que la transmission du code se fasse en temps réel. Il est fréquent que la communication des détails d'une transaction commerciale ne se fasse

pas en temps réel. C'est particulièrement vrai pour les transactions effectuées à l'étranger à l'aide d'une carte de paiement. Il y a aussi beaucoup de solutions proposées qui introduisent des détails comme le montant de la transaction dans l'algorithme ou encore qui encodent le numéro de transaction pour qu'il ne puisse être intercepté lors de la transmission. Tout cela amène un délai dans le traitement de la transaction: si le numéro envoyé pour identification contient des variables comme le temps, le montant etc., cela oblige l'institution réceptrice à décoder ce numéro avant d'autoriser la transaction. Comme le nombre de transactions simultanées est très important, un simple délai de quelques dixièmes de secondes rend son traitement beaucoup plus complexe et dispendieux que celui nécessaire pour valider les NIP actuels.

Les technologies enseignées dans les brevets déjà en vigueur ont aussi le désavantage de n'être utilisables qu'avec une seule institution à la fois. Cela entraîne inévitablement une augmentation importante du prix de revient pour l'implantation de ces procédés.

En somme, les solutions existantes comportent plusieurs limitations, désavantages et inconvénients qui les empêchent de répondre efficacement aux besoins d'identification courants d'un utilisateur et aux exigences des organismes adhérents. Notamment, ces solutions ne permettent pas de desservir à la fois plusieurs organismes de diverses natures, de sorte qu'en plus d'échouer à rendre plus sécuritaire les achats effectués avec une carte de crédit de façon pratique et acceptable pour le marché, elles s'avèrent inaptes à identifier un utilisateur dans plusieurs secteurs d'activités.

OBJETS DE L'INVENTION

Un objet de la présente invention est de fournir un appareil et une méthode d'identification surmontant les limites et inconvénients discutés ci-dessus.

Un second objet de la présente invention est que plusieurs institutions puissent se servir du même appareil pour diminuer de façon très importante les coûts d'implantation.

Un autre objet de l'invention est qu'un même appareil puisse fournir tous les codes d'identification variable (CIV) permettant d'identifier formellement son détenteur lors des démarches qu'il effectue auprès de plusieurs organismes adhérents.

Un autre objet de l'invention est que la méthode n'exige pas l'installation de nouveaux terminaux et fonctionne avec ceux déjà en place.

RÉSUMÉ DE L'INVENTION

D'après un premier aspect de l'invention, il est fourni un appareil fournissant un numéro de transaction unique et différent pour chaque utilisation de son détenteur, comprenant : une carte munie de touches et d'un écran; un circuit électronique intégré dans la carte ; et un programme faisant fonctionner le circuit électronique de façon à recevoir un code entré à l'aide des touches de la carte par le détenteur et affichant le numéro de transaction unique à l'écran.

Il est à noter que l'appareil peut être une carte à puce qui se connecte à un terminal qui comprend les touches et l'écran nécessaire, le terminal étant au point de transaction ou d'identification.

D'après un deuxième aspect de l'invention, un appareil d'identification universel permettant à une partie utilisatrice de s'identifier formellement auprès d'une seconde partie est proposé, ledit appareil d'identification universel comprenant : a) un dispositif d'entrée de données; b) un dispositif de sélection de la seconde partie parmi une pluralité de secondes parties auprès desquelles ladite partie utilisatrice peut s'identifier; c) un dispositif de sortie de données, et ; d) un dispositif de traitement de données comprenant un dispositif de mémorisation et un algorithme, et permettant de générer un code d'identification variable (CIV) spécifique à une utilisation donnée par la partie utilisatrice et de le révéler au moyen dudit dispositif de sortie de données.

D'après un troisième aspect de l'invention, une méthode d'identification universelle permettant à une partie utilisatrice de s'identifier formellement auprès d'une seconde partie au moyen d'un appareil d'identification est proposée, ladite méthode comprenant: a) sélectionner une seconde partie parmi une pluralité de secondes parties potentielles enregistrées dans l'appareil et auprès desquelles ladite partie utilisatrice peut s'identifier; b) entrer une donnée propre à la partie utilisatrice dans l'appareil; c) obtenir un code d'identification variable (CIV) spécifique à l'utilisation en cours calculé par l'appareil; d) communiquer à la seconde partie ledit code d'identification variable (CIV); et e) analyser ledit code d'identification variable communiqué à la seconde partie dans le but de vérifier une identité de la partie utilisatrice.

D'après un quatrième aspect de l'invention, une méthode d'identification universelle permettant à une partie utilisatrice de s'identifier formellement auprès d'une seconde partie au moyen d'un appareil d'identification est proposée, ladite méthode comprenant: a) ouvrir un dossier auprès de ladite seconde partie, comprenant enregistrer audit dossier un numéro d'identification personnel (NIP) propre à la partie utilisatrice et obtenir de la seconde partie au moins une donnée propre à ladite seconde partie; b) enregistrer dans ledit appareil le NIP propre à la partie utilisatrice et au moins une des données propres à la seconde partie, enregistrées audit dossier; c) utiliser l'appareil pour obtenir un code d'identification variable (CIV) permettant à la seconde partie de vérifier l'identité de la partie utilisatrice, comprenant sélectionner une seconde partie parmi une pluralité de secondes parties potentielles auprès desquelles un dossier a été ouvert et dont les données propres ont été enregistrées dans l'appareil et entrer un NIP dans l'appareil; et d) communiquer à la seconde partie ledit code d'identification variable.

D'après un cinquième aspect de l'invention, une méthode d'identification universelle permettant à une partie utilisatrice de s'identifier formellement auprès d'une seconde partie au moyen d'un appareil d'identification est proposée, ladite méthode comprenant: a) ouvrir un dossier auprès de ladite seconde partie, comprenant obtenir au moins une donnée propre à ladite seconde partie; b) enregistrer dans ledit appareil au moins une des données propres à la seconde partie, enregistrées audit dossier; c) enregistrer dans ledit appareil une donnée biométrique propre à la partie utilisatrice; d) utiliser l'appareil pour obtenir un code d'identification variable (CIV) permettant à la seconde partie de vérifier l'identité de la partie utilisatrice, comprenant sélectionner une seconde partie parmi une pluralité de secondes parties potentielles auprès desquelles un dossier a été ouvert et dont les données propres ont été enregistrées dans l'appareil et entrer dans l'appareil une donnée biométrique; et, e) communiquer à la seconde partie ledit code d'identification variable (CIV).

La méthode d'identification proposée repose sur la fourniture à une seconde partie (ci-après nommé : organisme adhérent), d'un code d'identification variable (CIV) de plus ou moins 5 caractères qui est unique et différent pour chacune des utilisations de l'utilisateur ou première partie (ci-après nommé: détenteur) de l'appareil. Comme ce CIV est valide pour une seule utilisation, l'interception de cette donnée n'est d'aucune

importance car pour qu'une autre utilisation puisse être valablement effectuée, il faut y adjoindre un tout nouveau CIV.

BRÈVE DESCRIPTION DES DESSINS

Relativement aux dessins qui illustrent la réalisation de l'invention.

La figure 1 représente une vue de face (en plan) de l'appareil (1) en accord avec la présente invention ;

La figure 2 représente une vue de face de l'appareil (1) intégrant un lecteur (11) d'empreinte digitale, conformément à un mode de réalisation alternatif de la présente invention;

La figure 3 représente une vue de face de l'appareil (1) intégrant des touches (12) permettant de sélectionner un organisme adhérent, conformément à un mode de réalisation alternatif de la présente invention;

La figure 4 représente une vue de face de l'appareil (1) intégrant un clavier numérique conventionnel (13) et des touches (12) permettant de sélectionner un organisme adhérent, conformément à un mode de réalisation alternatif de la présente invention;

La figure 5 représente une vue de face de l'appareil (1) intégrant un transducteur(15) servant de microphone ou de haut-parleur servant à l'entrée et à la sortie de données, conformément à un mode de réalisation alternatif de la présente invention.

La figure 6 représente un diagramme du fonctionnement du microprocesseur(14) intégré dans les appareils (1) des figures 1, 3 et 4, conformément à un mode de réalisation alternatif de la présente invention.

La figure 7 représente un diagramme de fonctionnement du microprocesseur(14) intégré dans les appareils (1) des figures 2 et 5, conformément à un mode de réalisation alternatif de la présente invention.

La figure 8 représente un diagramme de la méthode utilisée par le détenteur pour l'utilisation des appareils (1) des figures 1, 3 et 4, conformément à un mode de réalisation alternatif de la présente invention.

La figure 9 représente un diagramme de la méthode utilisée par le détenteur pour l'utilisation des appareils (1) des figures 2 et 5, conformément à un mode de réalisation alternatif de la présente invention.

La figure 10 représente un diagramme de la méthode générale utilisée pour tous les modèles (figs. 1, 2, 3, 4 et 5) d'appareil (1) lors de l'identification du détenteur, conformément à un mode de réalisation alternatif de la présente invention.

La figure 11 représente un diagramme des opérations d'un processus d'identification en accord avec un mode de réalisation alternatif de la présente invention.

DESCRIPTION DÉTAILLÉE DES MODES DE RÉALISATION ILLUSTRÉS

Les éléments similaires des différentes figures des illustrations jointes sont identifiés par les mêmes numéros de référence.

Nous allons maintenant décrire en détail les modes de réalisations préférés de l'appareil et du procédé de la présente invention en référant aux dessins ci-joints.

En se référant au dessin de la figure 1, on voit que l'appareil (1) est constitué d'un boîtier (1), de la dimension d'une carte d'identité traditionnelle quoiqu'un peu plus épais, qui inclut entre autre un microprocesseur (14), une source d'énergie qui peut être une batterie, un capteur d'énergie solaire. Ce boîtier peut être de forme rectangulaire, comme on le voit à la figure 1 ou de toute autre forme. Ce boîtier comporte un écran (2) afficheur, les chiffres (3) 1,2,3,4,5,6,7,8,9,0 imprimés autour de l'écran (2) et cinq touches (4,5,6,7,8) qui sont les suivantes : Une touche(6) portant l'inscription «power» servant à la mise en fonction de l'appareil(1); Une touche (7) portant l'inscription «enter» étant la touche servant à la validation et à l'enregistrement des données; Une touche (8) portant l'inscription «clear» étant la touche servant à l'annulation de la dernière donnée validée; Une touche (5) portant comme inscription une flèche servant à diriger le curseur (9) vers la droite de l'écran (2); Une touche (4) portant comme inscription une flèche servant à diriger un curseu (9) vers la gauche de l'écran (2);

Le dessin à la figure 2 représente un autre modèle d'appareil(1). Pour ce modèle, l'identification du détenteur ne se fait pas en entrant un NIP, elle se fait plutôt par la lecture d'une empreinte digitale. À cet effet un mini lecteur (11) d'empreinte digitale est intégré sur la façade de l'appareil(1). Le microprocesseur (14) enregistre l'empreinte digitale numérisée de son détenteur lors de la première activation de

l'appareil (1). Par la suite l'identification du détenteur se fait en comparant (72) l'empreinte digitale numérisée du doigt qui est placé sur le mini lecteu r(11) avec celle dans la mémoire du microprocesseur(14) de l'appareil (1). Si elles sont identiques, alors l'appareil émet (67, 75) le CIV (10) pour le dossier désiré.

Le dessin de la figure 3 représente un modèle d'appareil (1) qui est comparable à celui de la figure 1. La différence réside dans l'intégration d'un clavier (12) supplémentaire permettant de choisir directement, en appuyant sur la touche (12) appropriée, le dossier parmi ceux qui ont été préalablement activés.

Le dessin de la figure 4 représente un appareil (1) ne comportant pas de clavier sécurisé (4, 5). Celui-ci est remplacé par un clavier numérique (13) standard. Cet appareil (1) est également muni d'un clavier (12) servant à choisir directement, en appuyant sur la touche (12) appropriée, le dossier parmi un certain nombre préalablement activé.

Le dessin de la figure 5 représente un appareil (1) muni d'un transducteur (15) servant de microphone ou de haut-parleur, donc à l'entrée et à la sortie de données. On le met en fonction en appuyant sur la touche (16). L'appareil (1) est en mode d'entrée de données lorsque la touche (16) talk est enfoncée, l'entrée de donnée se fait verbalement par l'utilisateur. La sortie de donnée se fait également verbalement par le haut-parleur lorsque la touche (16) n'est pas enfoncée.

La figure 6 représente un diagramme du fonctionnement des appareils (1) fonctionnant avec l'identification du détenteur par la fourniture d'un NIP (figs.1,3,4). L'appareil (1) est mis en marche en pressant (51) la touche « power »(6) alors débute une utilisation (61). Le détenteur choisi l'organisme adhérent (62), ensuite le détenteur entre son NIP (63). Le microprocesseur (14) compare (64) le NIP entré avec le NIP en mémoire (14). Si le NIP entré est différent du NIP mémorisé (68) alors l'appareil (1) redemande d'entrer (63) le NIP, après trois tentatives infructueuses l'appareil (1) se ferme. Pour pouvoir réactiver l'appareil (1) le détenteur doit entrer un code spécial fourni par l'organisme adhérent. Si le NIP entré est identique (65) au NIP mémorisé alors le microprocesseur (14) génère(66) un code d'identification variable (CIV) (10) spécifique à l'utilisation en cours en utilisant le NIP entré (63), un code de référence (82) et un code de validation (83) propre à l'organisme adhérent pour modifier une combinaison tirée d'une table de combinaisons résidant dans l'appareil (1). Le code d'identification variable (CIV) (10) est révélé (67) au moyen du dispositif de sortie de

données (2). L'utilisateur presse (52) la touche « power »(6) pour terminer l'utilisation et fermer(69) l'appareil(1).

La figure 7 représente un diagramme du fonctionnement des appareils(1) fonctionnant avec l'identification du détenteur par la fourniture d'une donnée biométrique (figs.2 et 5). L'appareil (1) est mis en marche en pressant (51) la touche « power »(6 ou 16) alors débute une utilisation (61). Le détenteur choisit l'organisme adhérent (62), ensuite le détenteur fournit une donnée biométrique (71). Le microprocesseur(14) compare (72) la donnée avec celle en mémoire (14). Si la donnée biométrique fournie (71) est différente de celle mémorisé(74) alors l'appareil (1) redemande de fournir (71) la donnée biométrique, après trois tentatives infructueuses l'appareil (1) se ferme. Pour pouvoir réactiver l'appareil (1) le détenteur doit entrer un code spécial fourni par l'organisme adhérent. Si la donnée biométrique fournie est identique(73) à celle mémorisée alors le microprocesseur (14) génère (75) un code d'identification variable (CIV)(10) spécifique à l'utilisation en cours en utilisant un code de référence (82) et un code de validation (83) propre à l'organisme adhérent pour modifier une combinaison tirée d'une table de combinaisons résidant dans l'appareil (1). Le code d'identification variable (CIV) (10) est révélé (67) au moyen du dispositif de sortie de données (2,15). L'utilisateur presse (52) la touche « power »(6) pour terminer l'utilisation et fermer (69) l'appareil (1).

La figure 8 représente un diagramme illustrant les étapes nécessaires pour l'ouverture d'un dossier (80) jusqu'à la transmission (89) d'un code d'identification variable(CIV) (10) pour les appareils (1) (figs.1, 3 et 4) identifiant le détenteur par la fourniture (63) d'un NIP. Pour l'ouverture d'un dossier auprès d'un organisme adhérent le détenteur de l'appareil(1) enregistre (81) auprès de cet organisme un numéro d'identification personnel (NIP). Cet organisme émet un code de référence (82) et un code de validation (83) propre à cet organisme pour cet utilisateur. Le détenteur de l'appareil (1) active un dossier dans son appareil (1) pour cet organisme. Il lui attribue(84) un caractère d'identification. Il y enregistre (84.1) son numéro d'identification personne l(NIP). Il enregistre (85) dans son appareil (1) le code de référence (82) et le code de validation (83) propre à l'organisme. Pour obtenir un code d'identification variable (CIV) (10) le détenteur doit à l'aide de son appareil (1) sélectionner (86) un organisme adhérent, entrer son NIP (87) de cette façon il obtient (88) de son appareil (1) un code d'identification variable (CIV) (10). Il communique (89)

ce code d'identification variable (CIV) (10) à l'organisme adhérent pour lui permettre de vérifier son identité.

La figure 9 représente un diagramme illustrant les étapes nécessaires pour l'ouverture d'un dossier (90) jusqu'à la transmission (89) d'un code d'identification variable (CIV) (10) pour les appareils (1) (figs. 2 et 5) identifiant le détenteur par la fourniture (71) d'une donnée biométrique. Pour l'ouverture d'un dossier auprès d'un organisme adhérent, cet organisme émet un code de référence (82) et un code de validation 83) propre à cet organisme pour cet utilisateur. Le détenteur de l'appareil (1) active un dossier dans son appareil (1) pour cet organisme. Il lui attribue (84) un caractère d'identification. Il y enregistre (91) une donnée biométrique. Il enregistre (85) dans son appareil (1) le code de référence (82) et le code de validation (83) propre à l'organisme. Pour obtenir un code d'identification variable (CIV) (10) le détenteur doit à l'aide de son appareil (1) sélectionner (86) un organisme adhérent, entrer (92) la donnée biométrique, de cette façon il obtient (88) de son appareil (1) un code d'identification variable (CIV) (10). Il communique (89) ce code d'identification variable (CIV) (10) à l'organisme adhérent pour lui permettre de vérifier son identité.

La figure 10 représente un diagramme du déroulement (100) général d'une identification. Le détenteur doit tout d'abord mettre son appareil(1) en marche(101), sélectionner (86) et valider (102) un organisme adhérent avec le dispositif d'entrée de données (4, 5, 7, 8, 11, 12, 13, 15). Selon le modèle d'appareil (1) qu'il a en sa possession, il doit(figs.1, 3 et 4) entrer (103) et valider (104) son NIP ou pour les appareils des figures 2 et 5, entrer (92) une donnée biométrique au moyen du dispositif (11 et 15) approprié. Après validation (65 ou 73) l'appareil (1) éme (88) un code d'identification variable (CIV) (10). L'utilisateur communique (89) ce CIV (10) à l'organisme adhérent. Celui-ci en fait l'analyse (105), si le CIV (10) fourni (89) est valide (106) alors l'identification du détenteur par l'organisme adhérent est validée (108). Si le CIV (10) transmit (89) est erroné (107) alors l'organisme adhérent rejette l'identification du détenteur.

La figure 11 est un schéma simplifié démontrant une procédure d'autorisation selon la présente invention pour une transaction commerciale avec une carte de paiement. Le détenteur de l'appareil (1) apporte son achat au caissier du magasin. Comme il décide de payer le prix d'achat avec sa carte de paiement, il la prend et la remet au caissier. Le caissier la saisit et comme à l'habitude l'introduit dans un lecteur

de bande magnétique pour établir la communication (111) après avoir inscrit les détails nécessaires à la transaction comme le montant du prix de vente. La communication s'opère selon les protocoles en vigueur. L'organisme adhérent vérifie (112) la validité de ces données. Si les données sont validées (113) alors la transaction peut continuer, sinon (114) la transaction est annulée (116). Une fois cette étape terminée, l'institution financière émettrice de la carte de paiement demande (115) le code d'identification variable (CIV) (10) du détenteur. Le détenteur à l'aide de son appareil(1) sort(115) un code d'identification variable (CIV) (10). Il transmet (89) ce CIV (10). L'organisme adhérent valide (105) ce CIV (10). S'il est erroné (107), la transaction est annulée (118). Si le CIV (10) transmit (89) est valide (106) alors la transaction est autorisée.

L'appareil (1) et la méthode (100) ont pour but l'identification de son détenteur lors de démarches qu'il effectue auprès d'organismes qui ont adhérés à ce service. L'identification se fait à l'aide d'un code appelé «code d'identification variable (CIV (10)». Celui-ci est unique et différent pour chaque utilisation, il est valide pour une seule utilisation et remplacé par un autre CIV (10) lors d'utilisation ultérieure. Ce code d'identification variable(CIV) (10) est fourni par l'appareil (1) et révélé (67) à son détenteur au moyen du dispositif de sortie de données(2, 15). Le même appareil (1) sert à identifier son détenteur dans plusieurs situations de la vie quotidienne comme lors : de démarches auprès de son employeur, du gouvernement, de transactions avec une carte de paiement(crédit ou débit) ou de transaction avec tout autre organisme adhérent. Pour ce faire l'appareil (1) traite plusieurs dossiers qui pourront être attribués (84) par son détenteur à autant d'organismes différents.

L'appareil (1) a un dispositif de sortie de données (2,15) et un dispositif d'entrée de données (4, 5, 7, 8, 9, 11, 12, 13, 15) permettant à son détenteur une utilisation tout à fait sécuritaire. Pour avoir un code d'identification variable(CIV) (10), le détenteur s'identifie en entrant (103, 104) un numéro d'identification personnel (NIP) ou une donnée (92) biométrique (figs. 2,5) qui peut être: son empreinte digitale, son empreinte vocale etc., selon le modèle qu'il a en sa possession.

L'appareil (1) fonctionne de concert avec les autres pièces d'identité de son détenteur, telles que carte d'assurance sociale, cartes de crédit et de débit, permis de conduire, passeport etc. Selon le degré de sécurité exigé par l'organisme adhérent, le code d'identification variable (CIV) (10) est demandé occasionnellement ou de façon systématique.

L'appareil(1) émet pour son détenteur un code d'identification variable (CIV) (10) différent pour chacune de ses utilisations, que ce soit pour un même organisme ou pour un organisme différent.

Le code d'identification variable (CIV) (10) fourni par l'appareil (1) est transmis (89) par son détenteur à l'organisme adhérent de façon manuelle à l'aide des technologies déjà existantes servant à transmettre les NIP: comme les terminaux chez les commerçants, les guichets automatiques et les ordinateurs déjà en place. C'est la raison qui nous a amené à proposer un CIV (10) d'environ cinq caractères pour qu'il soit du même format que les NIP qui sont utilisés présentement.

Le détenteur de l'appareil (1) s'identifie (92, 103, 104) pour pouvoir utiliser son appareil (1). Selon le modèle (figs.1, 2 et 5) d'appareil (1) choisi, cette identification se fait soit en entrant un numéro d'identification personnel (NIP) (103, 104) ou en fournissant une donnée biométrique(92). Pour cette dernière méthode, au moment de la première activation de son appareil (1), le détenteur, enregistre (91) cette donnée biométrique, qui est emmagasinée dans la mémoire du microprocesseur (14) de son appareil (1). Seule la fourniture de la même donnée biométrique permettra l'émission d'un code d'identification variable(CIV) (10). De cette façon nous évitons le problème d'atteinte à la vie privée occasionnée par la fourniture et la détention de données biométriques par plusieurs organismes. Avec notre méthode (100), la donnée biométrique n'est fournie et détenue qu'à l'intérieur de l'appareil (1) de son détenteur et puisqu'il faut la fournir pour obtenir le bon code d'identification variable (CIV) (10), la transmission du bon CIV(10) vient nous identifier formellement. Pour les autres modèles (figs.1, 3, 4) d'appareils (1), il faut pour pouvoir se servir de l'appareil(1) entrer un numéro d'identification personnel (NIP) (87) à l'aide du dispositif d'entrée de données (4, 5, 7, 8, 9, 13).

Un autre modèle (fig.4) a un clavier numérique(13) standard permettant l'entrée du NIP (87) et des autres données numériques. Les modèles ici répertoriés ne sont pas limitatifs.

L'appareil (1) fonctionne à l'aide d'un microprocesseur (14) qui agit comme gestionnaire de dossiers et émetteur de CIV (10) à l'aide d'un algorithme. Le rôle de l'appareil (1) est de fournir un code d'identification variable(CIV) (10) différent pour chacune des demandes faites par son détenteur. À partir d'un algorithme commun à tous les appareils (1), le calcul (66, 75) pour fournir ce CIV (10) unique est fait en tenant

compte de deux données numériques (85) spécifiques à chacun des dossiers et pour chacun des détenteurs: un code référence (82) et un code de validation (83). Chacun de ces codes (82, 83) est fourni par l'organisme adhérent. Une troisième donnée, soit le NIP, choisi par le détenteur et enregistré (81) auprès de l'organisme adhérent, a également un rôle à jouer dans l'algorithme pour fournir le bon CIV (10). Pour les modèles (figs. 2 et 5) travaillant avec une donnée biométrique, l'algorithme ne tient compte que des deux données numériques (82, 83) spécifiques fournies par l'organisme adhérent pour générer les codes d'identification variable(CIV) (10).

Voici selon la méthode privilégiée le fonctionnement général de l'algorithme, il y a dans tous les appareils une table de base contenant 10 rangées. Chacune de ces rangées est composée d'un code de 12 chiffres. Cette table de base est présente 5 fois dans les appareils pouvant traiter 5 dossiers et 15 fois pour les appareils pouvant traiter 15 dossiers etc. Chacun des dossiers fonctionne indépendamment des autres dossiers.

Selon la méthode privilégiée, l'organisme adhérent fourni un code de référence qui a également 12 chiffres. Il fournit également un code de validation de 2 chiffres. Le détenteur de l'appareil (1) enregistre ces deux données dans son appareil (1) à l'aide du dispositif d'entrée de données. Une fois ces données enregistrées, l'algorithme fait les opérations suivantes : Indépendamment chacune des 10 rangées de la table de base contenant un code de 12 chiffres, viendra s'additionner au code de référence de 12 chiffres fourni par l'organisme adhérent. Cette opération se répète un nombre de fois égale à la valeur du code de validation. Si le code de validation est 14, alors chacun des 10 codes de 12 chiffres de la table de base vient s'additionner 14 fois au code de référence. Après chacune de ces additions, si le résultat donne un nombre de 13 chiffres, le premier chiffre qui est toujours «1» est éliminé pour ne conserver que les 12 derniers chiffres. Cette opération a pour but de modifier complètement la table de base, qui devient la table modifiée, c'est celle-ci qui sert à générer les codes d'identification variable(CIV) (10). Un appareil (1) ayant 11 dossiers actifs, a, après cette opération, 11 tables complètement différentes pour la sélection des codes d'identification variable(CIV)(10) de chacun des dossiers.

À partir de ce point, la façon de choisir les chiffres qui composent les CIV (10) est identique d'un dossier à l'autre et d'un appareil à l'autre. La seule exception est pour les appareils (1) qui fonctionnent avec un NIP pour identifier son détenteur, pour eux une autre opération mathématique est effectuée à l'aide du NIP pour modifier le code

d'identification variable (10). C'est ce CIV (10) modifié qui est révélé par le dispositif de sorties.

Selon la méthode privilégiée, la sélection du premier CIV (10) pour un dossier donné se fait sur la première rangée de la table modifiée. La deuxième sélection se fait sur la deuxième rangée etc. jusqu'à la dixième sélection qui se fait sur la dixième rangée. Pour la onzième sélection, nous revenons à la première rangée, mais avant qu'elle n'est lieu, la table modifiée sera modifiée une autre fois, comme pour la première modification, les codes de 12 chiffres contenus dans chacune des 10 rangées sont additionnés de nouveau au code de référence, qui est composé lui aussi de 12 chiffres. De cette façon une rangée contenue dans une table modifiée ne sert qu'une seule fois pour la sélection d'un code d'identification variable(CIV) (10) et elle sera modifiée avant de servir de nouveau.

Des modes de réalisation alternatifs de l'algorithme peuvent inclure des éléments variables «temps» qui sont générés par un dispositif d'horloge électronique intégré au microprocesseur (14). Ces éléments variables «temps» peuvent être soit l'heure et/ou la date. D'autres éléments variables peuvent être ajoutés, comme le montant d'un achat ou une situation géographique sans modifier la portée de cette invention.

Les organismes adhérents, ayant dans leur système informatique le même algorithme et connaissant les trois données spécifiques tel que décrit dans la présente demande, peuvent générer les CIV (10) de leur client et autorise r(108) une transaction après avoir validé (106) le code d'identification variable (CIV) (10) fourni (88) par l'appareil (1) de leur client et transmis (89) par celui-ci. Pour ce faire, ils effectuent le même calcul (105) que celui effectué par l'appareil (1) pour le client. L'organisme adhérent, pour ne pas augmenter le temps de traitement, peut même générer (105) un certain nombre de codes d'identification variable (CIV (10) à l'avance. L'organisme adhérent connaissant les clients détenant les appareils(1) fonctionnant avec les données biométriques (figs. 2, 5), ne tient compte, pour ces clients seulement, que des deux données numériques spécifiques (82, 83) qu'elle lui a elle-même transmis pour générer les CIV (10) correspondants.

Selon le mode de réalisation privilégié, l'organisme adhérent peut selon le degré de sécurité souhaité travailler avec une série plus ou moins longue de code d'identification variable (CIV) (10) qu'il a généré à l'avance. Une institution financière

peut avoir en attente 10 CIV (10) pour chacun de ses clients. Cela lui permet de valider un CIV (10) qui n'est pas nécessairement le prochain sur la liste à être fourni normalement. Cela peut arriver, entre autre, lorsqu'un client demande un CIV (10) avant d'effectuer une transaction et qu'il décide, au dernier moment, de ne pas effectuer cette transaction. Donc ce CIV (10) ne parvient jamais à l'institution financière et lorsque le même client effectue une autre transaction avec la même carte de paiement, son appareil(1) lui fournit un CIV (10) différent et le transmet à son institution financière. L'institution financière qui reçoit le deuxième CIV (10) peut autoriser cette transaction car elle a les 10 prochains CIV (10) de son client en mémoire. Selon sa volonté, elle peut éliminer le premier CIV (10) qui est sur sa liste ou le conserver un certain temps pour être certaine que ce CIV (10) n'a pas été utilisé dans une transaction qui ne lui a pas été transmise en temps réel. Cette façon de faire donne que 10 possibilités sur 10,000 pour trouver le bon CIV (10).

Par contre un employeur, par exemple un gestionnaire d'aéroport international, qui contrôle l'accès à des locaux hautement sécuritaires, peut décider de n'accepter que le prochain CIV (10) de son employé. Si celui-ci transmet un CIV (10) autre que le prochain sur la liste se voit interdire l'accès au local désiré. Pour pouvoir y accéder, il doit rentrer en contact avec son employeur pour prouver son identité. Chacun des organismes adhérents peut ainsi adapter ce système à ses propres besoins.

Le consommateur transmet(89) ce CIV (10) manuellement avec les claviers qui font déjà partie de nos vies, comme les terminaux chez les commerçants, les guichets automatiques, les téléphones à clavier et les nombreux ordinateurs qui nous entourent.

Puisque le CIV (10) est transmis manuellement, ce nouveau procédé fonctionne aussi bien pour des transactions conventionnelles avec cartes de crédit ou de débit sans devoir implanter des terminaux d'une nouvelle génération, que pour les transactions sur Internet ainsi que celles effectuées par téléphone. Il peut, comme nous l'avons vu, être utilisé pour les transactions effectuées avec un organisme gouvernemental, son employeur ainsi qu'avec des sites Internet pour avoir accès à des pages contrôlées etc.

Comment fonctionne le clavier sécurisé (4, 5, 6, 7, 8) (figs.1, 2 et 3). Contrairement à ce qui se fait à l'heure actuelle, le clavier (4, 5, 6, 7, 8) qui sert à enregistrer (84.1, 85) les données essentielles (code de référence (82), code de validation (83) fournies par l'organisme adhérent, NIP etc.) dans l'appareil (1) n'est pas

numérique. Ce clavier sécurisé (4 ,5, 6, 7, 8) est une autre innovation de cet appareil (1). Il est composé principalement de deux touches identifiées par deux flèches (4, 5). Ces touches (flèches) (4,5) servent à déplacer un curseur (9) apparaissant à l'écran (2) de l'apparei (1). Une touche(flèche)(4) pour diriger le curseur (9) vers la gauche et une autre touche (flèche) (5) pour le diriger vers la droite.

Bien sûr, il y a d'autres touches sur l'appareil (1). Ces autres touches sont respectivement : «power»(6) pour la mise en marche de l'appareil (1), «ENTER»(7) pour valider et enregistrer une entrée et «CLEAR»(8) pour annuler la dernière entrée. Regardons comment les touches (4,5) de l'appareil (1) rendent les transactions beaucoup plus sécuritaires.

Un utilisateur a déjà activé un dossier dans son appareil (1). Il est chez un commerçant et veut effectuer une transaction. Il met en marche l'appareil(1) en appuyant (51) sur la touche «power»(6). Alors apparaît à l'écran (2) «dossier #» avec un curseur (9) sous le chiffre (3) 1. Puisque l'utilisateur n'a qu'un dossier(organisme adhérent) activé dans son appareil (1), il presse immédiatement sur la touche «ENTER»(7) pour confirmer qu'il veut un code d'identification variable (CIV) (10) pour le dossier numéro «1». Apparaît alors à l'écran (2) de son appareil(1) «NIP» et un curseur (9). Ce curseur (9) est situé en dessous ou au-dessus d'un des chiffres(3) imprimés autour de l'écran (2) : «1 2 3 4 5 6 7 8 9 0 »(3). Pour une sécurité maximale, le curseur(9) n'apparaît jamais en dessous ou au-dessus du même chiffre (3). Il peut apparaître en dessous du 1 et la fois suivante apparaître, de façon aléatoire, en dessous du 5 ou au-dessus du 8 etc.

Pour notre exemple le NIP de l'utilisateur est 6384. Le curseur (9) est apparu en dessous du chiffre (3) 2. Puisque le premier chiffre composant le numéro du NIP est le 6, l'utilisateur appuie quatre fois sur la flèche de droite(5) pour amener le curseur(9) au-dessus du chiffre (3) 6. Il appuie sur la touche «ENTER»(7) pour valider et enregistrer ce premier chiffre.

Le curseur (9) disparaît momentanément de l'écran (2) et réapparaît sous ou au-dessus d'un autre chiffre (3), encore une fois ce chiffre (3) est choisi de façon aléatoire. Apparaît au même moment sur l'écran (2) un symbole comme celui-ci : «*» pour indiquer que le premier chiffre composant le NIP a été sélectionné. Bien sûr ce symbole «*» apparaîtra deux fois pour indiquer que les deux premiers chiffres du NIP ont été sélectionnés, ainsi de suite. Poursuivons notre exemple, le curseur(9) réapparaît

au-dessus cette fois du chiffre 9. L'utilisateur appuie donc à six reprises sur la flèche de gauche (4) pour amener le curseur(9) en dessous du chiffre(3) 3. Puisque le deuxième chiffre composant son NIP est bien le 3, il appuie sur la touche «ENTER»(7) pour valider et enregistrer ce chiffre. Le même processus recommence pour le choix du troisième et du quatrième chiffre de son NIP. S'il avait fait une erreur en appuyant sur le bouton «ENTER»(7) trop rapidement, il n'aurait qu'à presser la touche «CLEAR»(8) pour annuler la dernière entrée, faire la correction et poursuivre. Le curseur se positionne au haut de l'écran(2) pour les chiffres (3) 1,2,3,4,5 et au bas de l'écran (2) pour les chiffres (3) 6,7,8,9,0.

Avec cette nouvelle façon de faire, un fraudeur, même à l'affût, placé près de l'utilisateur ne peut le voir appuyer sur les chiffres composant son NIP. Tout ce qu'il voit, c'est l'utilisateur appuyant sur des flèches (4, 5) pour déplacer un curseur (9), qui lui, ne se positionne jamais en dessous ou au-dessus du même chiffre (3) pour débuter une nouvelle sélection, d'où une sécurité de transaction accrue.

Bien que la présente invention a été décrite avec les principales caractéristiques, il est prévu que différentes modifications peuvent être faites sans déroger à l'esprit et l'étendue de la présente invention. En conséquence, il est résolu que les caractéristiques décrites soient considérées seulement comme une illustration de la présente invention et que l'étendue de la présente invention ne devrait pas être limité à cela.

REVENDICATIONS :

1. Un appareil (1) fournissant un numéro de transaction (10) unique et différent pour chaque utilisation de son détenteur, comprenant :
une carte munie de touches (4,5,6,7,8) et d'un écran(2) ;
un circuit électronique intégré dans la carte ; et
un programme faisant fonctionner le circuit électronique de façon à recevoir un code entré à l'aide des touches(4,5,6,7,8) de la carte par le détenteur et affichant le numéro de transaction(10) unique à l'écran(2).

2. Un appareil (1) d'identification universel permettant à une partie utilisatrice de s'identifier formellement auprès d'une seconde partie, ledit appareil(1) d'identification universel comprenant :
   a) un dispositif d'entrée de donnée (4, 5, 7, 8, 9, 11, 12, 13, 15 et 16) ;
   b) un dispositif de sélection (4, 5, 7, 8, 9, 12, 13, 15 et 16) de la seconde partie parmi une pluralité de secondes parties auprès desquelles ladite partie utilisatrice peut s'identifier ;
   c) un dispositif de sortie (2 et 15) de données; et ;
   d) un dispositif de traitement (14) de données comprenant un dispositif de mémorisation et un algorithme (60 et 70), et permettant de générer un code d'identification variable (CIV) (10) spécifique à une utilisation donnée par la partie utilisatrice et de le révéler (67) au moyen dudit dispositif de sortie (2 et 15) de données.

3. Un appareil (1) d'identification universel tel que décrit à la revendication 2, caractérisé en ce que le dispositif d'entrée de données comprend un clavier(4, 5, 7, 8, 11, 12 et 13).

4. Un appareil (1) d'identification universel tel que décrit à la revendication 3, caractérisé en ce que ledit clavier comprend au moins une touche de sélection (4 et 5) de données, au moins une touche de validation(7) de donnée et au moins une touche d'effacement(8) de donnée.

5. Un appareil (1) d'identification universel tel que décrit à la revendication 2, caractérisé en ce que le dispositif d'entrée de données comprend un lecteur de données biométriques(11).

6. Un appareil (1) d'identification universel tel que décrit à la revendication 2, caractérisé en ce que ledit dispositif d'entrée de données comprend un microphone (15).

7. Un appareil (1) d'identification universel tel que décrit à la revendication 2, caractérisé en ce que ledit dispositif de sélection de la seconde partie comprend une pluralité de touches (12) dont chacune porte une inscription identifiant une des secondes parties de ladite pluralité de secondes parties.

8. Un appareil (1) d'identification universel tel que décrit à la revendication 2, caractérisé en ce que ledit dispositif de sortie de données comprend un affichage électronique visuel (2).

9. Un appareil (1) d'identification universel tel que décrit à la revendication 8, caractérisé en ce que ledit dispositif de sélection de la seconde partie comprend au moins une touche de sélection à défilement (4 et 5) permettant de faire apparaître successivement sur l'affichage une donnée d'identification correspondant à chacune de la pluralité de secondes parties, et une touche de validation (7) permettant de confirmer une sélection de la seconde partie.

10. Un appareil (1) d'identification universel tel que décrit à la revendication 8, caractérisé en ce que ledit dispositif d'entrée de données comprend un clavier comportant au moins une touche de sélectio (4, 5, 7, 8, 12 et 13) de données, au moins une touche de validation (7) de donnée et au moins une touche d'effacement (8) de donnée, et ledit affichage électronique visuel(2) est capable de coopérer avec ledit clavie r(4 et 5) pour permettre à la partie utilisatrice de composer et d'entrer dans l'appareil une séquence de caractères sans recourir à des touches de caractères et sans afficher ladite séquence de caractères.

11. Un appareil (1) d'identification universel tel que décrit à la revendication 2, caractérisé en ce que ledit dispositif de sortie de données comprend un dispositif de génération de signaux audibles (15).

12. Un appareil (1) d'identification universel tel que décrit à la revendication 2, caractérisé en ce que ledit dispositif de sélection de la seconde partie comprend un microphone (15) permettant de fournir verbalement une donnée d'identification de la seconde partie à sélectionner parmi la pluralité de secondes parties.

13. Un appareil (1) d'identification universel tel que décrit à l'une quelconque des revendications 3 et 4, caractérisé en ce que ledit clavier comprend des touches de caractères numériques (13).

14. Un appareil (1) d'identification universel tel que décrit à la revendication 5, caractérisé en ce que ledit lecteur de données biométriques comprend un lecteur d'empreintes digitales (11).

15. Un appareil (1) d'identification universel tel que décrit à la revendication 5, caractérisé en ce que ledit lecteur de données biométriques comprend un microphone(15).

16. Un appareil (1) d'identification universel tel que décrit à la revendication 2, caractérisé en ce que la génération dudit code d'identification variable (CIV) (10) par ledit dispositif de traitement (14) de données requiert au moins une donnée prédéterminée propre à la partie utilisatrice, obtenue au moyen dudit dispositif d'entrée, et au moins une donnée propre à la seconde partie, mémorisée dans ledit dispositif de mémorisation (14).

17. Un appareil (1) d'identification universel tel que décrit à la revendication 2, caractérisé en ce que ledit dispositif de traitement(14) de données génère ledit code variable (CIV) (10) à partir d'un numéro d'identification personnel (NIP) lui étant fourni à chaque utilisation par la partie utilisatrice au moyen dudit dispositif

(4, 5, 7, 8, 9, 13) d'entrée, et de deux séquences numériques propres à la seconde partie lesquelles résident en permanence dans ledit dispositif de mémorisation (14) après un enregistrement initial.

18. Un appareil (1) d'identification universel tel que décrit à la revendication 2, caractérisé en ce que ledit algorithme (60) comprend :

a) obtenir (62) l'identification de l'organisme adhérent pour l'utilisation en cours à partir d'un dispositif d'entrée(4, 5, 7, 8, 9, 12et 13) de données ;

b) obtenir (63) un *numéro d'identification personnel* (NIP) du dispositif d'entrée (4, 5, 7, 8, 9 et 13) de données;

c) comparer (64) ledit NIP à un numéro de référence mémorisé;

d) calculer (66) un code d'identification variable(CIV) (10) spécifique pour l'utilisation en cours si le NIP correspond (65) au numéro de référence, ledit calcul comprenant utiliser deux données propres à la seconde partie enregistrées (85) dans le dispositif de mémorisation (14), pour modifier une combinaison tiré d'une table de combinaisons prédéterminées résidant dans l'appareil et ainsi créer un nouveau code; et,

e) révéler (67) le nouveau code en tant que code d'identification variable(CIV)(10) spécifique à l'utilisation en cours.

19. Un appareil (1) d'identification universel tel que décrit à la revendication 2, caractérisé en ce que ledit algorithme (70) comprend :

a) obtenir(62) l'identification de l'organisme adhérent pour l'utilisation en cours, à partir d'un dispositif d'entrée (4, 5, 7, 8, 9 et 15) de données ;

b) obtenir (71) du dispositif d'entrée(11 et 15) de données une donnée biométrique propre à la partie utilisatrice;

c) comparer (72) ladite donnée biométrique avec une donnée de référence mémorisée;

d) calculer (75) un code d'identification variable(CIV (10) spécifique pour l'utilisation en cours si la donnée biométrique correspond (73) à celle de référence, ledit calcul comprenant utiliser deux données (85)

propres à la seconde partie enregistrées dans le dispositif de mémorisation (14), pour modifier une combinaison tirée d'une table de combinaisons prédéterminées résidant dans l'appareil et ainsi de créer un nouveau code; et,

e) révéle (67) le nouveau code en tant que code d'identification variable (CIV) (10) spécifique à l'utilisation en cours.

20. Un appareil (1) d'identification universel tel que décrit à la revendication 2, caractérisé en ce que ledit code d'identification variable (CIV) (10) comprend une combinaison de caractères et la pluralité de secondes parties auprès desquelles ladite partie utilisatrice peut s'identifier comprend au moins cinq secondes parties.

21. Une méthode d'identification universelle (100) permettant à une partie utilisatrice de s'identifier formellement auprès d'une seconde partie au moyen d'un appareil (1) d'identification, ladite méthode comprenant:

a) sélectionner(86) une seconde partie parmi une pluralité de secondes parties potentielles enregistrées dans l'appareil et auprès desquelles ladite partie utilisatrice peut s'identifier;

b) entrer (92, 103 et 104) une donnée propre à la partie utilisatrice dans l'appareil;

c) obtenir (88) un code d'identification variable (CIV) (10) spécifique à l'utilisation en cours calculé par l'appareil (1);

d) communiquer (89) à la seconde partie ledit code d'identification variable (CIV) (10) ; et

e) analyser (105) ledit code d'identification variable communiqué à la seconde partie dans le but de vérifier une identité de la partie utilisatrice.

22. Une méthode d'identification universelle (100) telle que décrite à la revendication 21, caractérisée en ce que, analyser (105) ledit code d'identification variable comprends comparer ledit code à une liste de codes prédéterminés.

23. Une méthode d'identification universelle (100) telle que décrite à la revendication 21, caractérisée en ce que, analyser (105) ledit code d'identification comprends calculer au moins un code d'identification au moyen d'un algorithme utilisant au moins une donnée propre à la partie utilisatrice et au moins une donnée propre à la seconde partie.

24. Une méthode d'identification universelle (100) telle que décrite à la revendication 21, caractérisée en ce que, entrer une donnée propre à la partie utilisatrice comprend entrer (103 et 104) un numéro d'identification personnel.

25. Une méthode d'identification universelle (100) telle que décrite à la revendication 24, caractérisée en ce que, entre r(103 et 104) un numéro d'identification personnel comprend utiliser un clavier (4, 5, 7 et 8) dépourvu de touches de caractères numériques.

26. Une méthode d'identification universelle (100) telle que décrite à l'une quelconque des revendications 24 et 25, caractérisée en ce que, entrer (103 et 104) un numéro d'identification personnel comprend faire défiler un curseur(9) vis-à-vis des caractères (3) imprimés sur une face de l'appareil (1) et presser une touche du clavier pour valider (7) la sélection de l'un desdits caractères (3) lorsque celui-ci est indiqué par ledit curseur (9).

27. Une méthode d'identification universelle (100) telle que décrite à la revendication 21, caractérisée en ce que, entrer une donnée propre à la partie utilisatrice comprend lire (92) une caractéristique biométrique.

28. Une méthode d'identification universelle (100) telle que décrite à la revendication 21, caractérisée en ce que sélectionner (86 et 102) une seconde partie potentielle comprend presser une touche (12) portant une inscription identifiant ladite seconde partie potentielle.

29. Une méthode d'identification universelle (100) telle que décrite à la revendication 21, caractérisée en ce que sélectionner (86) une seconde partie potentielle

comprend faire afficher successivement par l'appareil une pluralité d'identités de secondes parties potentielles enregistrées dans ledit appareil et valider (102) la sélection d'une seconde partie dont l'identité est affichée.

30. Une méthode d'identification universelle (100) telle que décrite à la revendication 21, caractérisée en ce que sélectionner (86 et 102) une seconde partie potentielle comprend dicter verbalement une information identifiant ladite seconde partie.

31. Une méthode d'identification universelle (100) telle que décrite à la revendication 21, caractérisée en ce que la partie utilisatrice peut s'identifier formellement auprès d'une seconde partie sans que lesdites données (92) propres à la partie utilisatrice soient communiquées à une tierce partie ou lues par un appareil détenu par celle-ci.

32. Une méthode d'identification universelle (100) telle que décrite à la revendication 21, caractérisée en ce que le code d'identification variable (CIV) (10) est traité comme un numéro d'identification personnel (NIP) par une tierce partie responsable d'obtenir une preuve d'identité pour le compte de la seconde partie.

33. Une méthode d'identification universelle (80) permettant à une partie utilisatrice de s'identifier formellement auprès d'une seconde partie au moyen d'un appareil (1) d'identification, ladite méthode comprenant:

a) ouvrir (81, 82 et 83) un dossier auprès de ladite seconde partie, comprenant enregistrer (81) audit dossier un numéro d'identification personnel (NIP) propre à la partie utilisatrice et obtenir(82 et 83) de la seconde partie au moins une donnée propre à ladite seconde partie;

b) enregistrer (84.1) dans ledit appareil le NIP propre à la partie utilisatrice et au moins une des données (85) propres à la seconde partie, enregistrées audit dossier;

c) utiliser l'appareil pour obtenir (88) un code d'identification variable (CIV) (10) permettant à la seconde partie de vérifier l'identité de la partie utilisatrice, comprenant sélectionner (86) une seconde partie parmi une

pluralité de secondes parties potentielles auprès desquelles un dossier a été ouvert et dont les données propres(85) ont été enregistrées dans l'appareil(1) et entrer(87) un NIP dans l'appareil; et,

d) communiquer(89) à la seconde partie ledit code d'identification variable.

34. Une méthode d'identification universelle (90) permettant à une partie utilisatrice de s'identifier formellement auprès d'une seconde partie au moyen d'un appareil (1) d'identification, ladite méthode comprenant:

a) ouvrir un dossier auprès de ladite seconde partie, comprenant obtenir (82 et 83) au moins une donnée propre à ladite seconde partie;

b) enregistrer (85) dans ledit appareil (1) au moins une des données propres à la seconde partie, enregistrées audit dossier;

c) enregistrer (91) dans ledit appareil (1) une donnée biométrique propre à la partie utilisatrice;

d) utiliser l'appareil (1) pour obtenir (88) un code d'identification variable (CIV) (10) permettant à la seconde partie de vérifier l'identité de la partie utilisatrice, comprenant sélectionner (86) une seconde partie parmi une pluralité de secondes parties potentielles auprès desquelles un dossier a été ouvert et dont les données (85) propres ont été enregistrées dans l'appareil et entrer (92) dans l'appareil une donnée biométrique; et,

e) communiquer (89) à la seconde partie ledit code d'identification variable (CIV) (10).

FIGURE 1

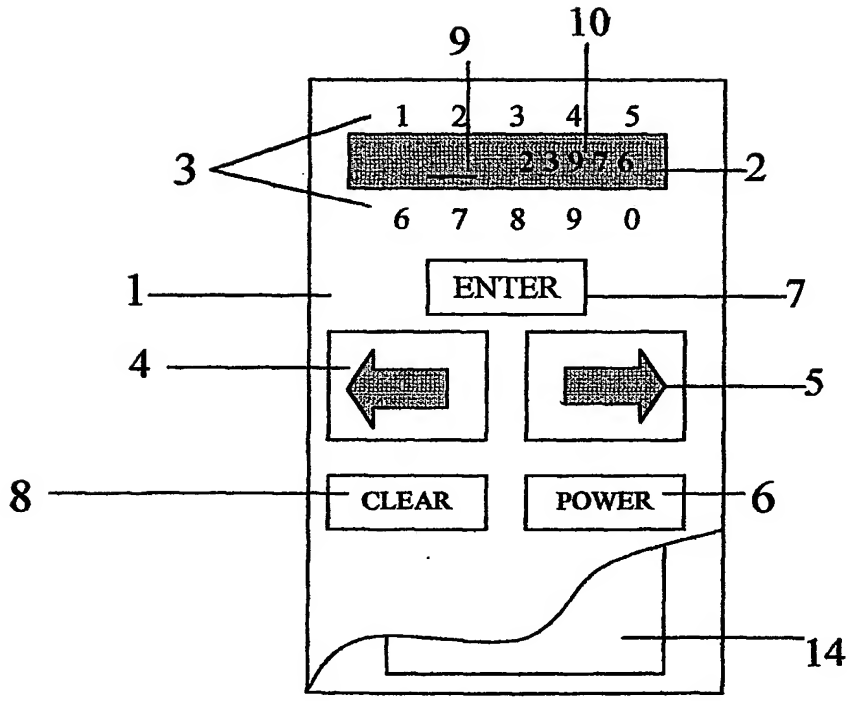


FIGURE 2

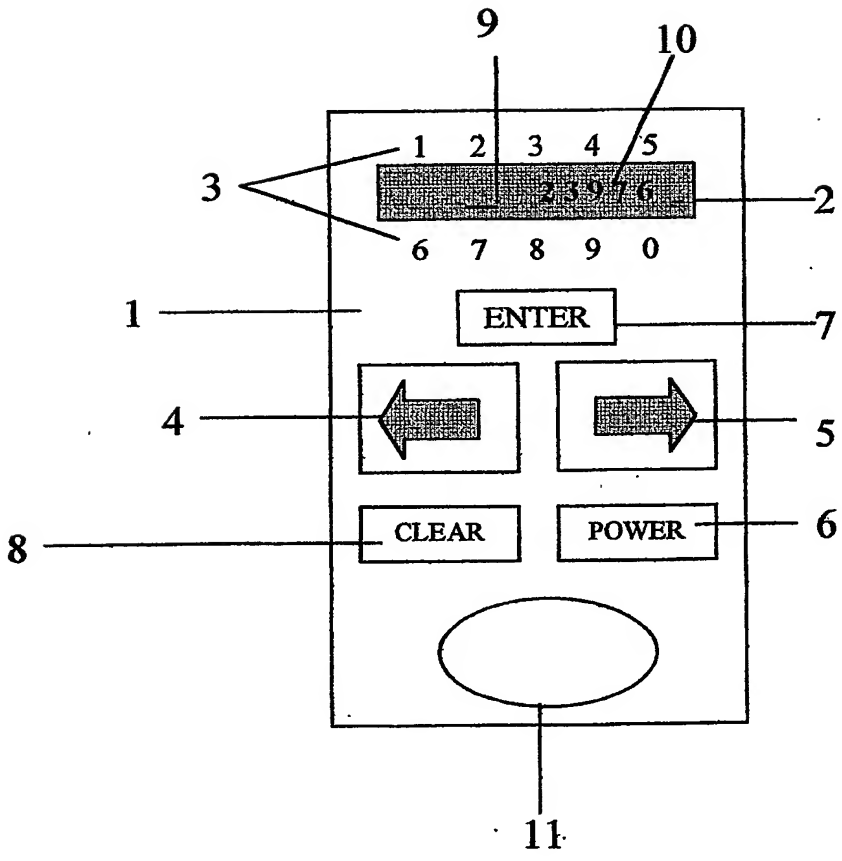


FIGURE 3

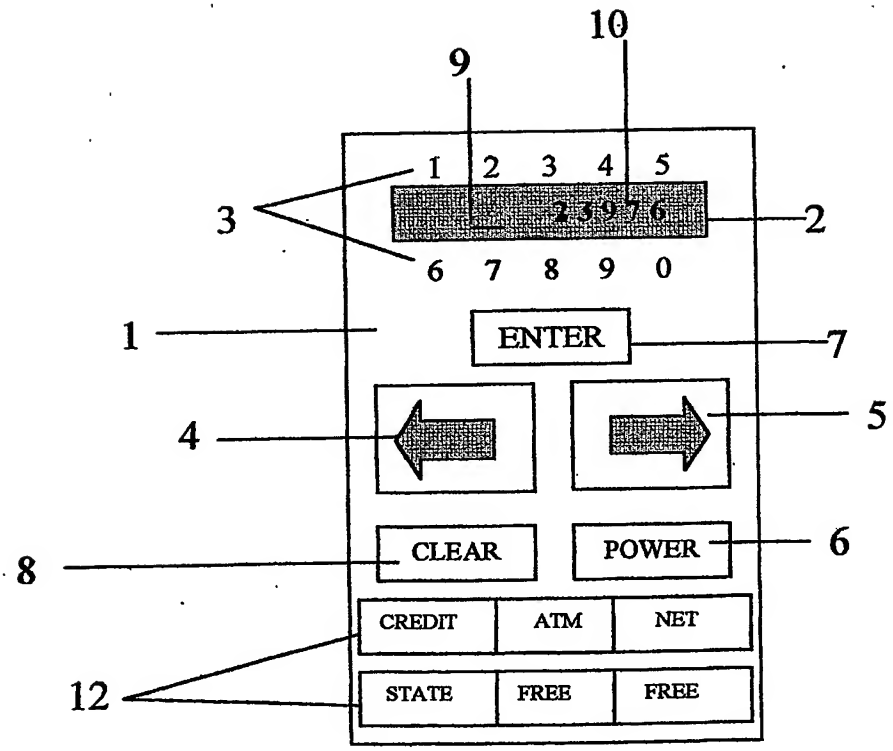

10
9
1 2 3 4 5
3
2 3 9 7 6
2
6 7 8 9 0
1
ENTER
7
4
5
8
CLEAR
POWER
6
CREDIT
ATM
NET
12
STATE
FREE
FREE

FIGURE 4

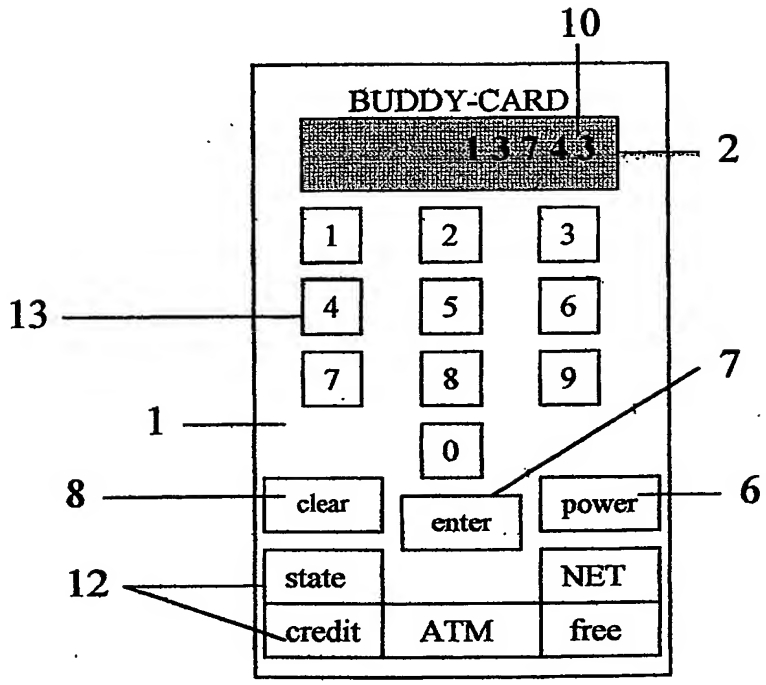

10
BUDDY-CARD
1 3 7 4 3
2
1
2
3
13
4
5
6
7
8
9
7
1
0
8
clear
enter
power
6
12
state
NET
credit
ATM
free

FIGURE 5

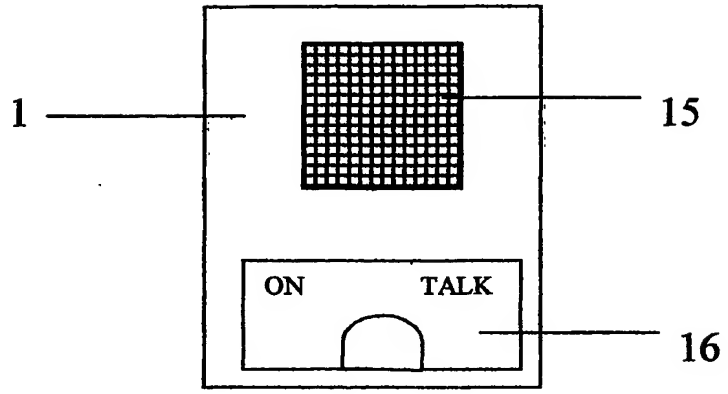


FIGURE 6

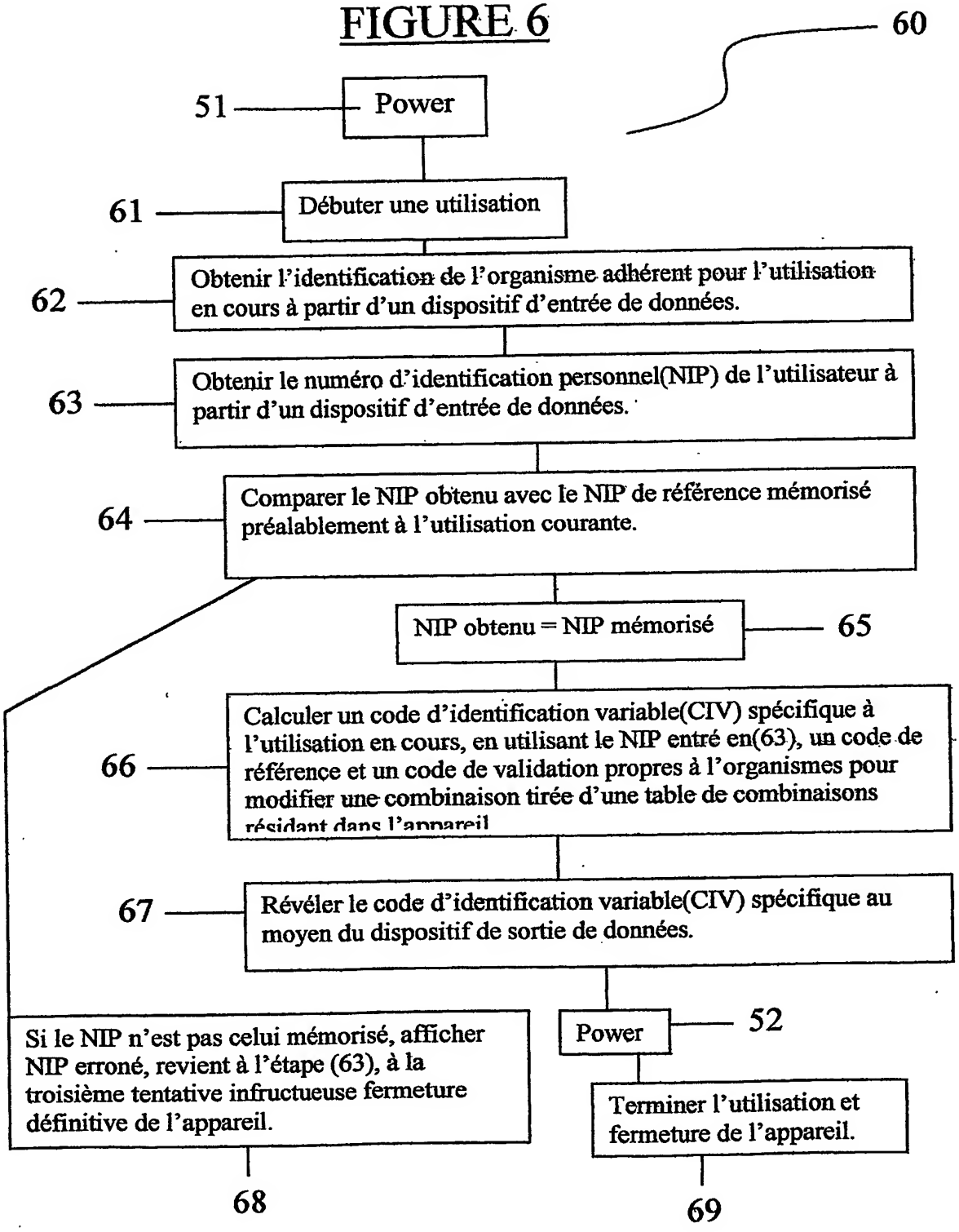

60
51
Power
61
Débuter une utilisation
62
Obtenir l'identification de l'organisme adhérent pour l'utilisation en cours à partir d'un dispositif d'entrée de données.
63
Obtenir le numéro d'identification personnel(NIP) de l'utilisateur à partir d'un dispositif d'entrée de données.
64
Comparer le NIP obtenu avec le NIP de référence mémorisé préalablement à l'utilisation courante.
NIP obtenu = NIP mémorisé
65
66
Calculer un code d'identification variable(CIV) spécifique à l'utilisation en cours, en utilisant le NIP entré en(63), un code de référence et un code de validation propres à l'organismes pour modifier une combinaison tirée d'une table de combinaisons résidant dans l'appareil
67
Révéler le code d'identification variable(CIV) spécifique au moyen du dispositif de sortie de données.
Si le NIP n'est pas celui mémorisé, afficher NIP erroné, revient à l'étape (63), à la troisième tentative infructueuse fermeture définitive de l'appareil.
Power
52
Terminer l'utilisation et fermeture de l'appareil.
68
69

FIGURE 7

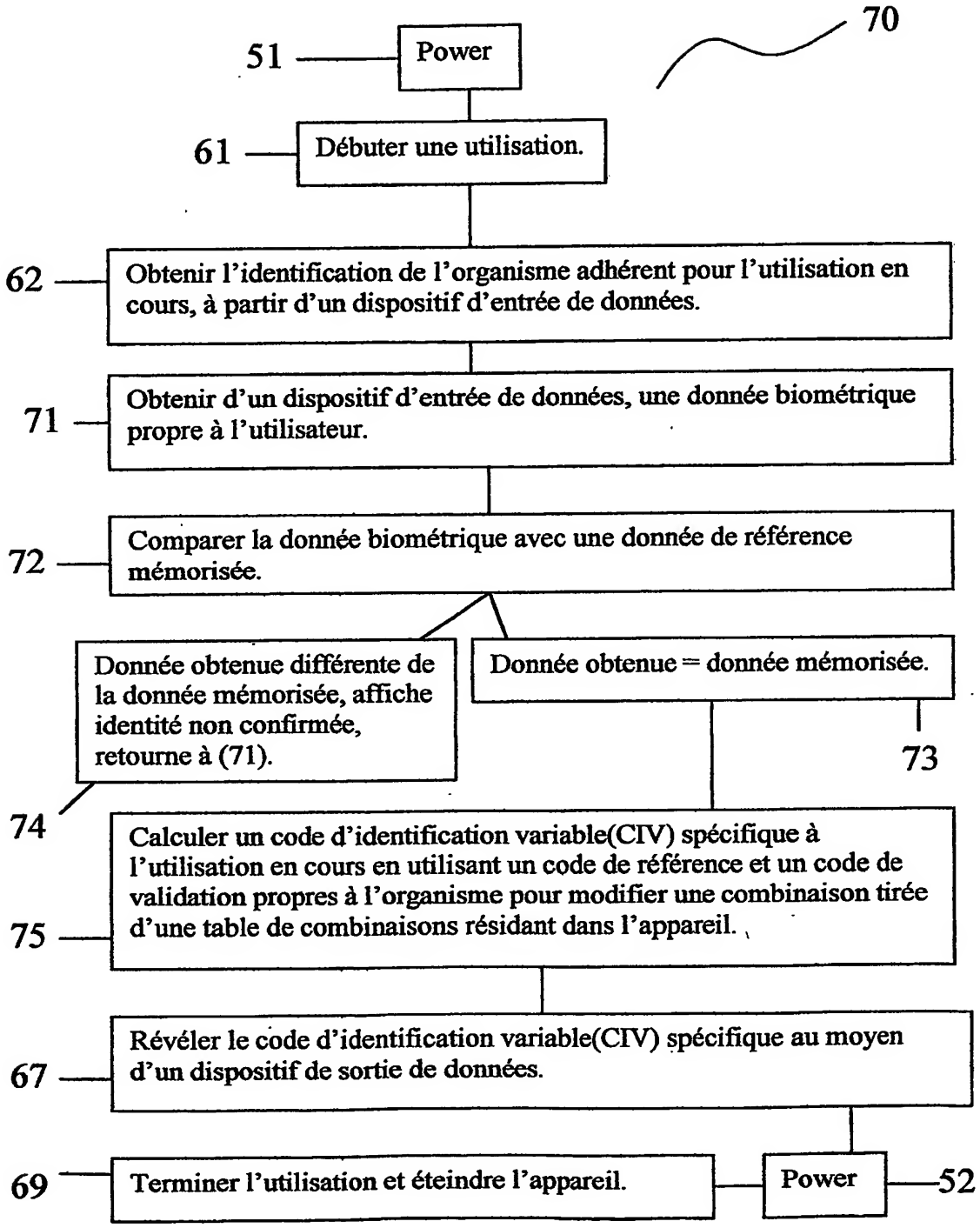

70
51
Power
61
Débuter une utilisation.
62
Obtenir l'identification de l'organisme adhérent pour l'utilisation en cours, à partir d'un dispositif d'entrée de données.
71
Obtenir d'un dispositif d'entrée de données, une donnée biométrique propre à l'utilisateur.
72
Comparer la donnée biométrique avec une donnée de référence mémorisée.
Donnée obtenue différente de la donnée mémorisée, affiche identité non confirmée, retourne à (71).
Donnée obtenue = donnée mémorisée.
73
74
Calculer un code d'identification variable(CIV) spécifique à l'utilisation en cours en utilisant un code de référence et un code de validation propres à l'organisme pour modifier une combinaison tirée d'une table de combinaisons résidant dans l'appareil.
75
Révéler le code d'identification variable(CIV) spécifique au moyen d'un dispositif de sortie de données.
67
69
Terminer l'utilisation et éteindre l'appareil.
Power
52

FIGURE 8

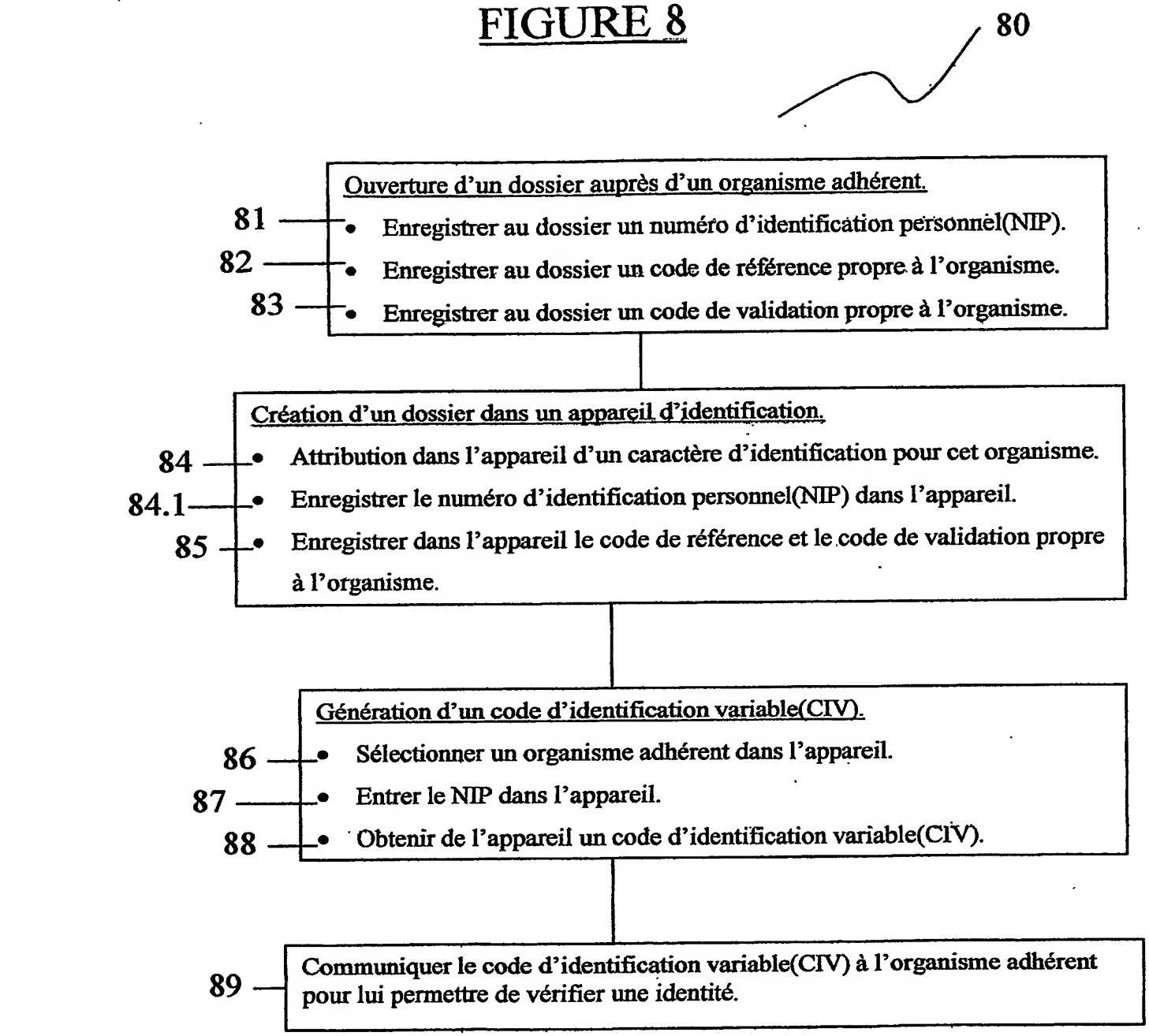

80
Ouverture d'un dossier auprès d'un organisme adhérent.
81
• Enregistrer au dossier un numéro d'identification personnel(NIP).
82
• Enregistrer au dossier un code de référence propre à l'organisme.
83
• Enregistrer au dossier un code de validation propre à l'organisme.
Création d'un dossier dans un appareil d'identification.
84
• Attribution dans l'appareil d'un caractère d'identification pour cet organisme.
84.1
• Enregistrer le numéro d'identification personnel(NIP) dans l'appareil.
85
• Enregistrer dans l'appareil le code de référence et le code de validation propre à l'organisme.
Génération d'un code d'identification variable(CIV).
86
• Sélectionner un organisme adhérent dans l'appareil.
87
• Entrer le NIP dans l'appareil.
88
• Obtenir de l'appareil un code d'identification variable(CIV).
89
Communiquer le code d'identification variable(CIV) à l'organisme adhérent pour lui permettre de vérifier une identité.

FIGURE 9

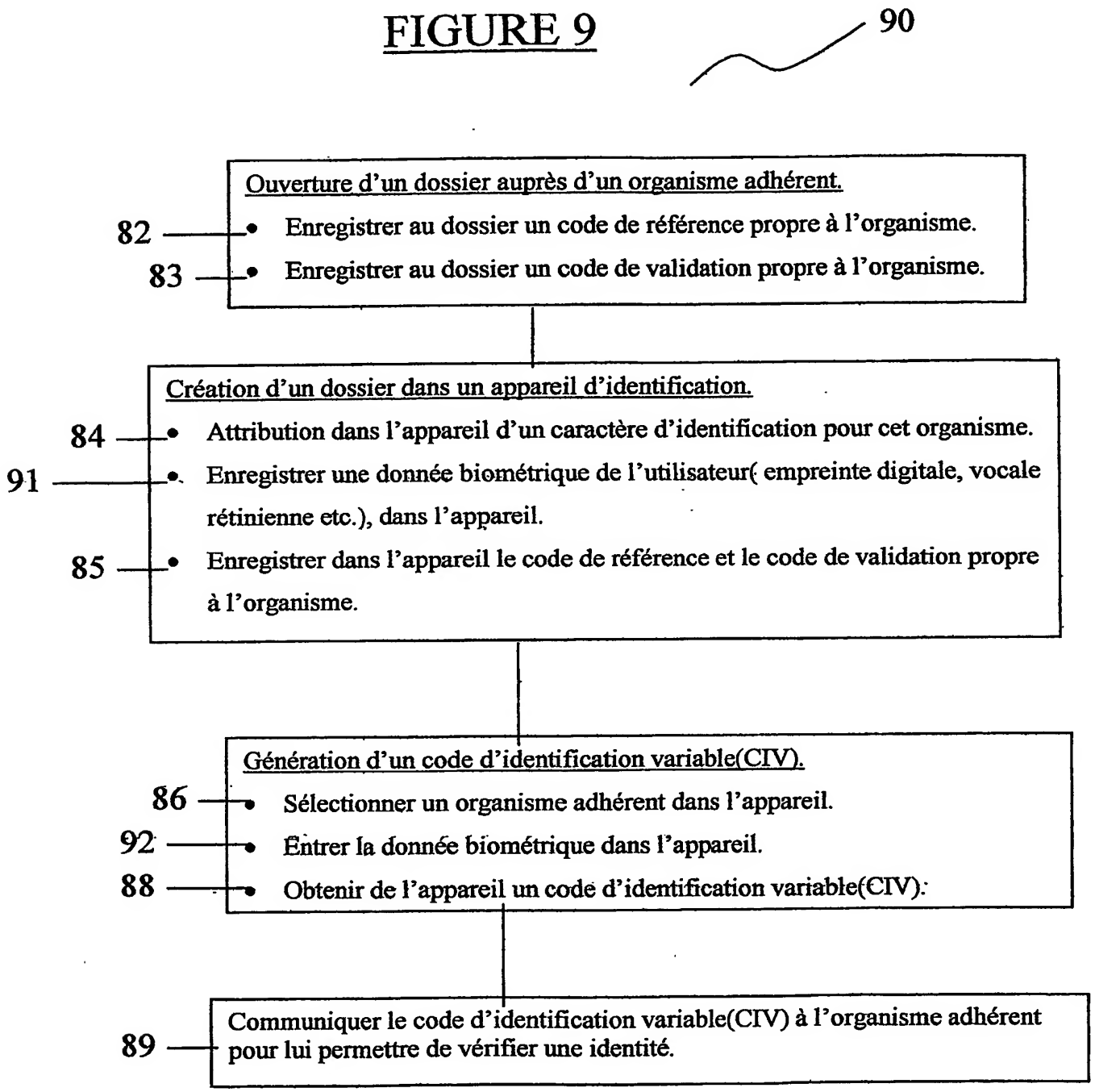
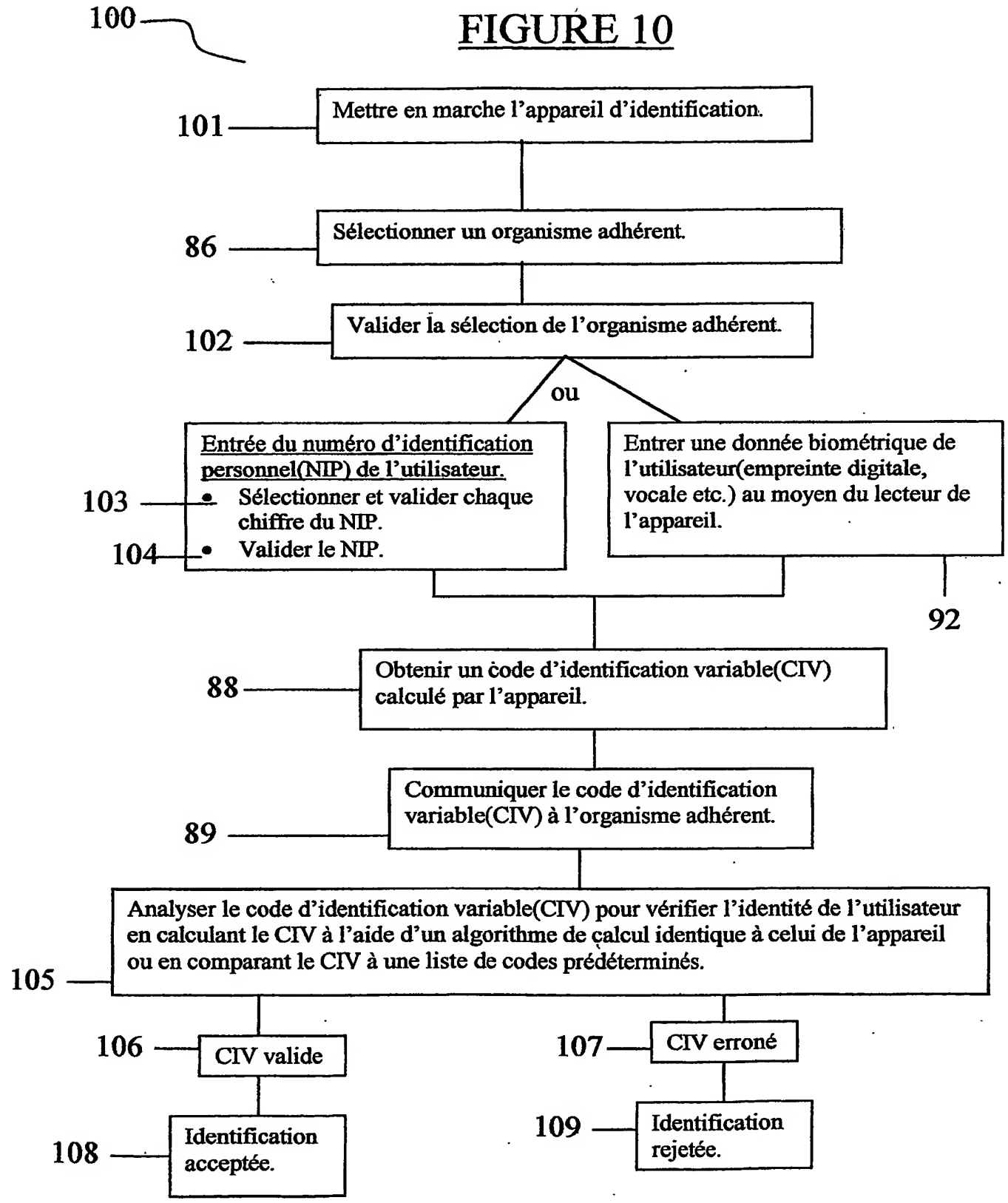

90
Ouverture d'un dossier auprès d'un organisme adhérent.
82
Enregistrer au dossier un code de référence propre à l'organisme.
83
Enregistrer au dossier un code de validation propre à l'organisme.
Création d'un dossier dans un appareil d'identification.
84
Attribution dans l'appareil d'un caractère d'identification pour cet organisme.
91
Enregistrer une donnée biométrique de l'utilisateur(empreinte digitale, vocale rétinienne etc.), dans l'appareil.
85
Enregistrer dans l'appareil le code de référence et le code de validation propre à l'organisme.
Génération d'un code d'identification variable(CIV).
86
Sélectionner un organisme adhérent dans l'appareil.
92
Entrer la donnée biométrique dans l'appareil.
88
Obtenir de l'appareil un code d'identification variable(CIV).
89
Communiquer le code d'identification variable(CIV) à l'organisme adhérent pour lui permettre de vérifier une identité.

FIGURE 10


100
101
Mettre en marche l'appareil d'identification.
86
Sélectionner un organisme adhérent.
102
Valider la sélection de l'organisme adhérent.
ou
Entrée du numéro d'identification personnel(NIP) de l'utilisateur.
103
Sélectionner et valider chaque chiffre du NIP.
104
Valider le NIP.
Entrer une donnée biométrique de l'utilisateur(empreinte digitale, vocale etc.) au moyen du lecteur de l'appareil.
92
88
Obtenir un code d'identification variable(CIV) calculé par l'appareil.
89
Communiquer le code d'identification variable(CIV) à l'organisme adhérent.
105
Analyser le code d'identification variable(CIV) pour vérifier l'identité de l'utilisateur en calculant le CIV à l'aide d'un algorithme de calcul identique à celui de l'appareil ou en comparant le CIV à une liste de codes prédéterminés.
106
CIV valide
107
CIV erroné
108
Identification acceptée.
109
Identification rejetée.

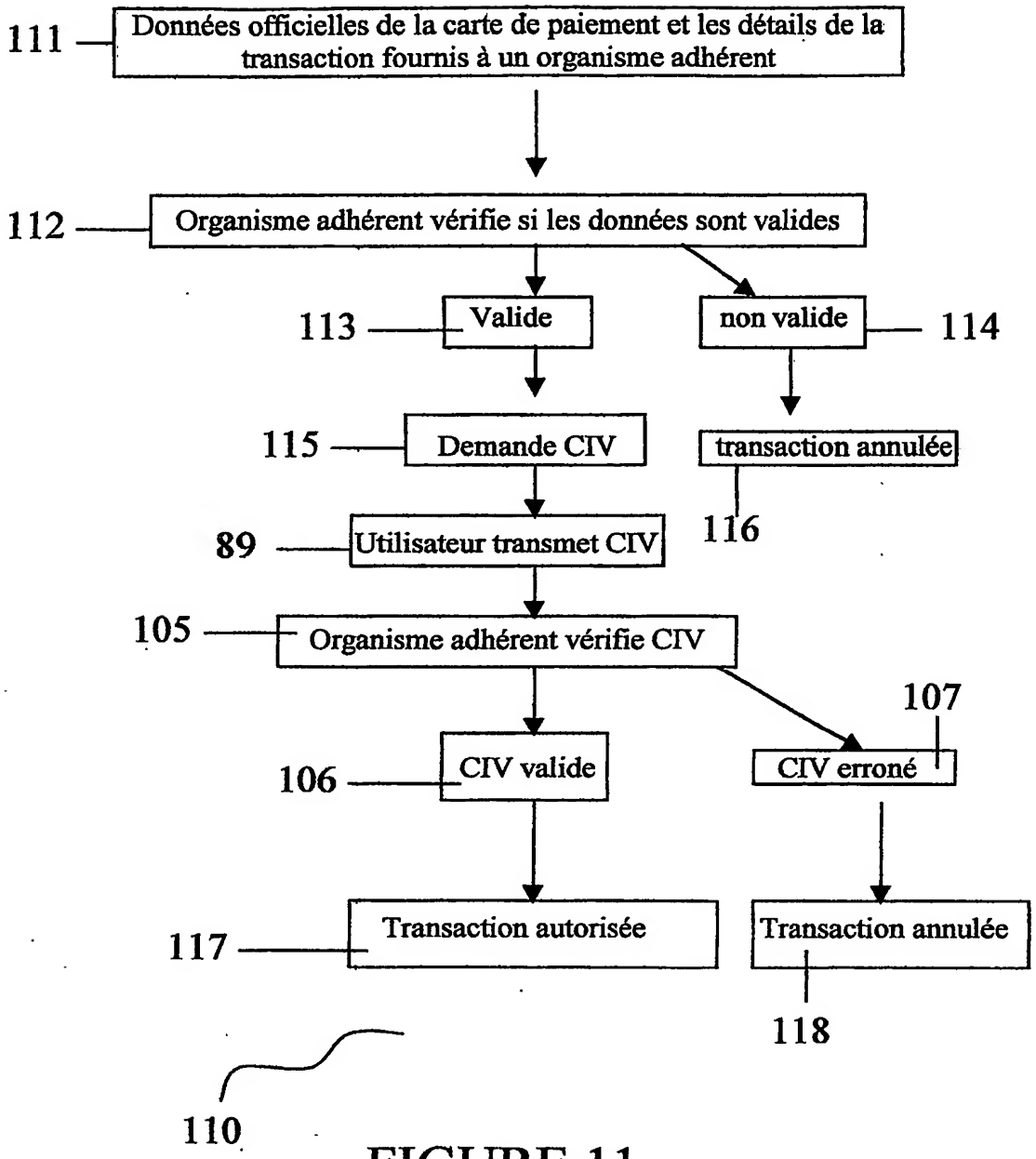

111
Données officielles de la carte de paiement et les détails de la transaction fournis à un organisme adhérent
112
Organisme adhérent vérifie si les données sont valides
113
Valide
non valide
114
115
Demande CIV
transaction annulée
116
89
Utilisateur transmet CIV
105
Organisme adhérent vérifie CIV
107
106
CIV valide
CIV erroné
117
Transaction autorisée
Transaction annulée
118
110

FIGURE 11